

Rec'd PCT/PTO 30 JAN 2006

10/500, 952

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date  
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number  
WO 2004/088483 A2

(51) International Patent Classification<sup>7</sup>: G06F 1/00 [GB/GB]; Star Internet, Brighouse Court, Barmwood, Gloucester GL4 3RT (GB).

(21) International Application Number: PCT/GB2004/000214 (74) Agents: AYERS, Martyn, Lewis, Stanley et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(22) International Filing Date: 19 January 2004 (19.01.2004)

(25) Filing Language: English (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(26) Publication Language: English

(30) Priority Data: 0307736.9 3 April 2003 (03.04.2003) GB

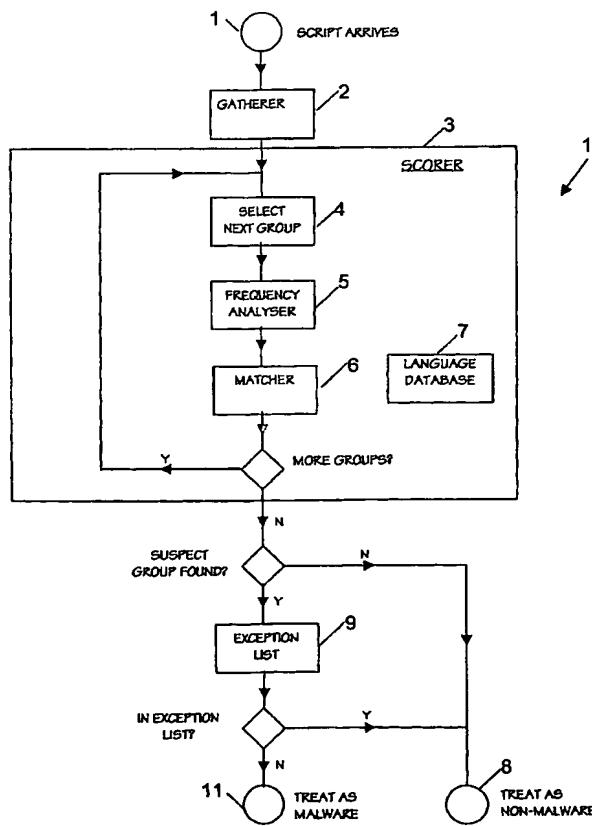
(71) Applicant (for all designated States except US): MESSAGELABS LIMITED [GB/GB]; 1270 Lansdowne Court, Gloucester Business Park, Gloucester GL3 4AB (GB).

(72) Inventor; and (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

(75) Inventor/Applicant (for US only): SHIPP, Alexander

[Continued on next page]

(54) Title: SYSTEM FOR AND METHOD OF DETECTING MALWARE IN MACROS AND EXECUTABLE SCRIPTS





Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

- *without international search report and to be republished upon receipt of that report*

## SYSTEM FOR AND METHOD OF DETECTING MALWARE IN MACROS AND EXECUTABLE SCRIPTS

5        The present invention relates to a method of, and system for, heuristically detecting malware in macros and executable scripts, by checking for the presence of encoded strings.

10      Viruses and other forms of malware (malicious software) pose an ever-increasing problem for computer users and users of the internet. Early viruses tended to be spread as binary executables which would execute on computers of a known type. A traditional measure against virus infections is anti-virus file scanning in which a file, treated as a succession of bytes, is scanned looking for byte patterns that have been identified as characteristic signatures of known malware. This virus scanning may take place on files stored on a local or network disk drive or files which are in transit on a network, with the scanning taking place as they pass by a particular node on the network or 15 pass through a network gateway such as an email gateway. Since the use of the internet for web access, email and other purposes has become widespread, and the software to be found on a typical user's machine has become more sophisticated, the opportunity has arisen for virus writers to create viruses which are distributed in essentially source code forms. These so-called script- or macro viruses rely on the user's computer having 20 software on it which will act as an execution environment for a program, that is the virus, which arrives at the computer e.g. as an email attachment.

25      Features added to an operating system to increase the ease of use by non-technical users offer opportunities for virus writers to exploit. For example, Microsoft Windows has a facility whereby files having a certain file extension (that is, the character(s) following the final "." in the file name) are associated with a particular application program such that the act of the user "opening" the file in Windows' graphical user interface causes Windows to activate the associated program and load the file in question. This has provided the basis for recent script viruses which work by attaching a 30 file containing the source code to an email which is then distributed to users; the file is given the extension necessary to activate the script host program on a recipient's computer. When the recipient opens the attachment, the host is activated and the files executed. There have been a number of virus outbreaks in which the virus is spread as a script for the Visual Basic Scripting host on Windows machines.

Similarly, a number of end-user applications such as word processors and spreadsheets incorporate a "macro" facility for enabling the user to automate repetitive or difficult tasks. The macro "language" involved may be of differing degrees of sophistication, with some, such as those found in Microsoft Office products, being very similar to parallel scripting languages. A minor difference is that scripts tend to be stored, on disk and elsewhere, purely in source code form, whereas macro files may include binary data as well as or instead of textual source code. For example, this binary data may include a "tokenised" version of the macro's source code, or actual executable machine codes.

10 In addition to Visual Basic Scripting and Microsoft Office macros, there are several computer languages where the source code is available in the executable file. This might be because the language is interpreted without being compiled, for example, Perl. Virus writers who use such mediums often try and make their creations hard to detect. They may do this writing code that is hard to understand. They may also write self 15 modifying code, so that with each generation of the code, the code subtly changes. This is done in order to make it hard for anti-virus vendors to create signatures that detect the virus in all its infinite variations. They may also hide virus code in comments or strings. These are then read in, decrypted, and acted upon.

20 Signature-based scanning is ineffective against script- and source-code-only macro viruses, because their contents do not correspond one-for-one with machine instructions, since there are many different ways the same programmatic action may be expressed in source code and source code may be transformed in various ways, for example in terms of usage of "whitespace", i.e., space, tab and newline characters, or substitution of variable names which will alter the contents of the source code without 25 altering its effect.

The present invention is based on an appreciation of the fact that, as regards script- and macro-viruses, in some of these cases, it is possible to heuristically detect the virus by frequency analysis of character counts in various parts of the program.

30 According to the present invention there is provided a system for scanning for malware a computer file containing source code of a computer program in a given computer language comprising:

means for separating the source code into groups of constituent parts corresponding to different structural parts of the program;

means for processing each part to count the number of occurrences in that part of characters of a character set to obtain a frequency distribution of characters in that part;

5 means for comparing the character frequency distribution of each part with an expected range of frequency distributions; and

means for flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means

The invention also provides a method for scanning for malware a computer file containing source code of a computer in a given computer program language  
10 comprising:

separating the source code into groups of constituent parts corresponding to different structural parts of the program;

processing each part to count the number of occurrences in that part of characters of a character set to obtain a frequency distribution of characters in that part;

15 comparing the character frequency distribution of each part with an expected range of frequency distributions; and

flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means.

The invention will be further described by way of non-limitative example  
20 with reference to the accompanying drawing, in which:-

Figure 1 is a combined block diagram of, and flow chart of the operation of, one embodiment of a system according to the present invention

The embodiment of the invention illustrated in Figure 1 is for use in an anti-virus scanning system, in which a succession of files are presented for scanning at an  
25 input 1, are subject to scanning by the system 10 and then flagged as possibly containing a virus depending on the result. The origin of the files is not material to the present invention: they may be files read in succession from a local or network disk-drive and may be the files ordinarily stored on the disk drive for its normal purpose or files which are created by the system to store attachments to e-mails being processed by a mail scanning  
30 system of which the system illustrated in Figures 1 forms part. It is assumed that the files applied to the input 1 have been subject to prior automatic filtering to filter out all those bar ones which are considered to be script files or macro files containing scripts.

The system 10, which may be implemented by means of a software automaton operates according to the following algorithm.

**Algorithm**

1. A script file is delivered to the input 1 for processing.
2. A 'gatherer' 2 analyses the program which the script defines and gathers together the program parts being analysed into groups, eliminating duplicates. Typical groups would be the group of all comments, the group of variable names, the group of subroutine names, the group of strings, but the invention is not limited to these particular groups.
3. The gathered group contents are then passed to a scorer 3, which will score each group as suspicious or not suspicious.
4. The scorer 3 selects the first group for processing at 4.
5. A frequency analyser 5 takes the contents of the group, counts the number of occurrences of each character, working out a frequency distribution histogram data set.
6. A matcher 6 takes this distribution from the analyser 5 and determines whether this has a close match with the distribution expected for the languages it knows about as recorded in a language database 7. If not, the group is provisionally flagged as suspect.
7. If there are groups left, go to step 4.
8. If there are no groups marked as suspect, finish processing by flagging the file to be treated as non-malware at an output 8.
9. The script is checked by an exception list matcher 9 to see if it can be ignored. This is, for instance, to ignore known scripts which flag as suspicious. If the script can be ignored, stop processing and flag the file to be treated as non-malware at output 8.
10. If processing arrives here, the script is flagged as malware, by activating a "treat as malware" flag at output 11.

**Gatherer**

One way of implementing gatherer 2 is as a process that parses the script, breaking it up into components. Components the system 10 is interested in, such as comments, strings and so on, are stored in groups for future analysis by the scorer 3. The gatherer 2 will need different parsing processes for different types of scripts. For instance, comments in PERL are introduced by the hash character, '#', while comments in Microsoft VBA (Visual BASIC for Applications) are introduced either by the word 'Rem', or by a single quote.

**Example**

The following is an example VBA script

```
5      Sub Test()
      Rem This is a test subroutine
      Rem It does not do much
      Rem MsgBox "Hello World"
      End Sub
10
10     Sub Test2()
      Rem This another routine
      Rem It does not do much
      Dim var As Integer
15
15     Dim AnotherVar as String
      Var = 7
      AnotherVar = "Hello"
      Var = Var + 3
      End Sub
20
```

This would generate the following groups:

**Group of comments**

```
25      This is a test subroutine
      It does not do much
      This another routine
```

**Group of routine names**

```
30      Test
      Test2
```

**Group of strings**

```
      Hello World
      Hello
```

**Group of variable names**

```
35      var
      AnotherVar
```

**Scorer**

The scorer 3 processes each group, and also consists of the frequency analyser and the matcher.

**Frequency Analyser**

45 The frequency analyser 5 converts upper case letters to the equivalent lower case letter. It then counts the number of instances of each character code in each group, and calculates percentages. Analysis is not confined to single byte character sets, that is the frequency analyser 5 should be adapted to handle multi-byte character sets and Unicode.

### Example:

If the group of strings is

Hello. World  
Hello

5

Then the frequency distribution will be

10	a 0	f 0	k 0	p 0	u 0	z	0
	b 0	g 0	l 5	q 0	v 0	space	1
	c 0	h 2	m 0	r 1	w 1		
	d 1	i 0	n 0	s 0	x 0		
	e 2	j 0	o 3	t 0	y 0		

15 and the percentage frequency distribution will be

a	0.00	f	0.00	k	0.00	p	0.00	u	0.00	z	0.00
b	0.00	g	0.00	l	31.25	q	0.00	v	0.00	space	6.25
c	0.00	h	12.50	m	0.00	r	6.25	w	6.25		
d	6.25	i	0.00	n	0.00	s	0.00	x	0.00		
e	12.50	j	0.00	o	18.75	t	0.00	y	0.00		

## Matcher

25 The matcher 6 compares the frequency distribution of the group as calculated by the frequency analyser 5, with the frequency distribution of known sets. Normally these sets will be written languages, such as English, German, Chinese and so on. Depending on the particular group, the matcher 6 may or may not take all or some punctuation into account. For instance, subroutine and variable names typically do not contain punctuation, and so punctuation will be ignored for these groups. However strings 30 and comments typically would contain punctuation – especially spaces, and so punctuation will not be ignored for these groups.

Matching is done set by set by comparing the percentage frequency for each character, with the expected percentage frequency range for that character. If the frequency falls outside the range, an anomaly is recorded, and a count incremented. Once all characters have been processed, the anomaly count is checked, and if greater than a certain value, the group is flagged as not matching the set. Processing then continues with the next set. If the anomaly count is not greater than the certain value, the group is flagged as matching the set, and processing stops with the matcher recording the group was not suspect.

40 If no sets match, the group is recorded as suspect.

The allowed percentage frequency range for each character will be a function of the set (e.g. English), the actual character (e.g. 'E') , and the total number of

characters in the group under test – a large group under test will be expected to have a better correlation than a small group. Sufficiently small groups are not expected to have good correlation ,and there will be a cut off point where the function returns the limits as between 0% and 100%.

5 The allowed anomaly count will be a function of the set and the total number of characters in the group under test.

For instance, in English the letter 'e' might be expected to occur roughly 10% of the time. For a group of size 10,000 the function might return expected limits of 9.2% and 10.8%. For a group of size 1,000, the limits might be 7% and 12.5%.

10

### **Exception List**

15

The exception list handler 9 implements rules which are used to eliminate false positives for known programs that are harmless but which may otherwise be accidentally marked as suspicious. The exception list rules can work in various ways, including but not limited to comparing the MD5 checksum of a file with a list of known checksums, or by searching the files for regular expressions. If an exception list match occurs, no further action is taken, beyond flagging the file as "treat as non-malware" at output 8.

20

Programs which are stopped as viral, but which do not turn out to be viral, can be analysed, and an exception list entry generated and added to the rules of exception list handler 9, so that similar false positives do not occur in future.

25

30

As well as using the system 10 as a stand-alone virus detection system, it can be combined with systems which implement other techniques as part of a larger system. For instance, programs flagged as viral by the system 10 may be allocated a certain score, or variety of scores depending on the exact circumstances, possibly to be taken into account in conjunction with scores taken from other systems. Different groups may be allocated different weightings (for instance, an anomaly in the group of strings may be more suspicious than an anomaly in the group of variables). Scores may also be assigned using other heuristic techniques, and only if the total score passes some limit is the program flagged as viral.

Extra long strings or arrays of strings may be considered as a separate group all by themselves.

Small sample sets may be ignored. For instance, if there are only ten variables, this may not be enough to analyse.

## CLAIMS

1. A system for scanning for malware a computer file containing source code of a computer program in a given computer language comprising:

5 means for separating the source code into groups of constituent parts corresponding to different structural parts of the program;

means for processing each part to count the number of occurrences in that part of characters of a character set to obtain a frequency distribution of characters in that part;

10 means for comparing the character frequency distribution of each part with an expected range of frequency distributions; and

means for flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means.

2. A system according to claim 1 wherein the flagging means is operative to flag the file as suspect if the comparing means detects that the frequency distribution of 15 one or more of said parts does not match an expected range.

3. A system according to claim 1 wherein the flagging means is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each part with an expected frequency distribution.

4. A system according to claim 1, 2 or 3 wherein, in operation of the 20 comparing means, the range of distributions which it considers as representing an acceptable match for the part is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

5. A system according to any one of the preceding claims and including:

means for maintaining an exception list of files which by their contents are 25 to be treated as exceptions;

means for identifying a file as being included in the exception list; and

wherein a file is not marked as suspect if it is identified as being on the exception list.

6. A system according to any one of the preceding claims wherein duplicates of parts are ignored.

7. A method for scanning for malware a computer file containing source code of a computer program in a given computer language comprising:

5 separating the source code into groups of constituent parts corresponding to different structural parts of the program;

processing each part to count the number of occurrences in that part of characters of a character set to obtain a frequency distribution of characters in that part;

10 comparing the character frequency distribution of each part with an expected range of frequency distributions; and

flagging the file as suspect or not depending on the result of one or more comparisons by the comparing means.

8. A method according to claim 7 wherein the flagging means is operative to flag the file as suspect if the comparing means detects that the frequency distribution of 15 one or more of said parts does not match an expected range.

9. A method according to claim 7 wherein the flagging means is operative to flag the file as suspect depending on an accumulated score prepared by adding individual scores obtained in comparing each part with an expected frequency distribution.

10. A method according to claim 7, 8 or 9 wherein, in operation of the 20 comparing means, the range of distributions which it considers as representing an acceptable match for the part is varied depending on the number of characters either in part or the program as a whole, with fewer characters corresponding to a wide range.

11. A method according to any one of claims 7 to 10 and including:  
25 maintaining an exception list of files which by their contents are to be treated as exceptions;

identifying a file as being included in the exception list; and  
wherein a file is not marked as suspect if it is identified as being on the exception list.

1/1

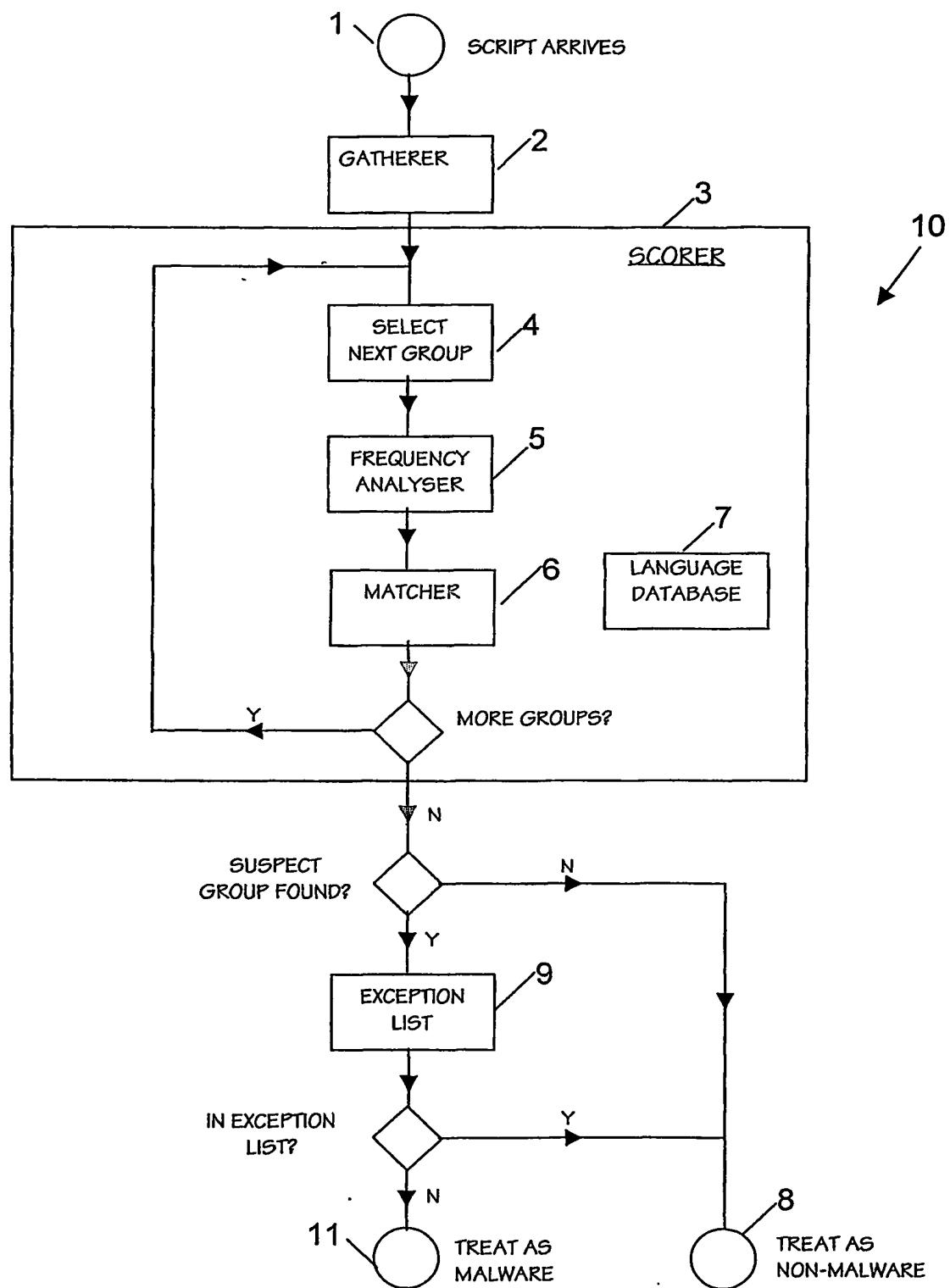


Fig.1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization International Bureau



(43) International Publication Date  
14 October 2004 (14.10.2004)

PCT

(10) International Publication Number  
WO 2004/088483 A3

(51) International Patent Classification<sup>7</sup>: G06F 1/00 [GB/GB]; Star Internet, Brighouse Court, Barmwood, Gloucester GL4 3RT (GB).

(21) International Application Number: PCT/GB2004/000214 (74) Agents: AYERS, Martyn, Lewis, Stanley et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(22) International Filing Date: 19 January 2004 (19.01.2004)

(25) Filing Language: English (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(26) Publication Language: English

(30) Priority Data: 0307736.9 3 April 2003 (03.04.2003) GB

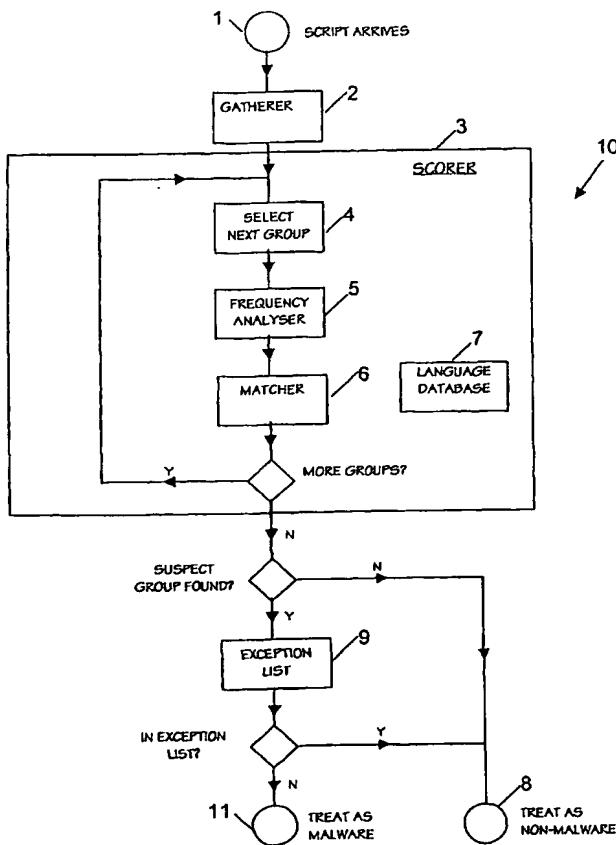
(71) Applicant (for all designated States except US): MESSAGELABS LIMITED [GB/GB]; 1270 Lansdowne Court, Gloucester Business Park, Gloucester GL3 4AB (GB).

(72) Inventor; and (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),

(75) Inventor/Applicant (for US only): SHIPP, Alexander

[Continued on next page]

(54) Title: SYSTEM FOR AND METHOD OF DETECTING MALWARE IN MACROS AND EXECUTABLE SCRIPTS



(57) Abstract: An anti malware scanner for files is provided with means for processing script and macro files and flagging them as suspect or not based upon an automated analysis of source code in the file. This analysis involves separating the program source into groups of parts such as comment, variable names and routine names, eliminating duplicates and performing a character frequency distribution analysis of the resulting strings. The system may include an exception list to omit flagging a file as suspect if it is on the exception list.

WO 2004/088483 A3



Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *with international search report*

**(88) Date of publication of the international search report:**

17 March 2005

## INTERNATIONAL SEARCH REPORT

Int'l Application No  
PCT/GB2004/000214A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 02/10888 A (BEETZ ANDREW ; CONTENT TECHNOLOGIES LTD (GB)) 7 February 2002 (2002-02-07) page 3, line 1 – page 4, line 30 page 8, line 21 – page 10, line 30 figure 2 -----	1-11
Y	WEBER M ET AL: "A toolkit for detecting and analyzing malicious software" PROCEEDINGS OF THE 18TH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 9 December 2002 (2002-12-09), pages 423-431, XP010627054 paragraphs '0003!, '03.1!, '03.3!, '03.4! ----- -/-	1-11

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

## \* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the International filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the International filing date but later than the priority date claimed

- \*T\* later document published after the International filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- \*&\* document member of the same patent family

Date of the actual completion of the International search

Date of mailing of the International search report

6 December 2004

13/12/2004

## Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patenttaan 2  
NL - 2280 HV Rijswijk  
Tel: (+31-70) 340-2040, Tx. 31 651 epo nl  
Fax: (+31-70) 340-3016

## Authorized officer

Segura, G

## INTERNATIONAL SEARCH REPORT

Inter I Application No  
PCT/GB2004/000214

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VELDMAN F: "COMBATING VIRUSES HEURISTICALLY" VIRUS BULLETIN CONFERENCE, VIRUS BULLETIN LTD., ABINGTON, GB, September 1993 (1993-09), pages 67-75, XP000828110 paragraphs '03.2!, '03.3! -----	5
A	US 2002/066024 A1 (KWAN TONY ET AL) 30 May 2002 (2002-05-30) abstract paragraphs '0011! - '0016! paragraph '0027! -----	1-4,7-10
A	US 5 907 834 A (SORKIN GREGORY BRET ET AL) 25 May 1999 (1999-05-25) column 2, line 45 - column 4, line 8 -----	1-4,7-10

## INTERNATIONAL SEARCH REPORT

Inte  
Application No  
PCT/GB2004/000214

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0210888	A 07-02-2002	GB 2365158	A 13-02-2002	
		AU 7571601	A 13-02-2002	
		EP 1305695	A2 02-05-2003	
		WO 0210888	A2 07-02-2002	
		US 2004236884	A1 25-11-2004	
US 2002066024	A1 30-05-2002	NONE		
US 5907834	A 25-05-1999	US 5675711	A 07-10-1997	